RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-SIX TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
JOHN DAVISSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

August 14, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 6

ARGUMENT 7

I. The world has changed since *Smith v. Maryland*. The widespread use of mobile phones and the routine collection of detailed location data was not possible in 1979. 11

A. The analog phone system in the 1970s did not generate "out of band" personal data. ... 11

B. The pen register in *Smith* recorded only the outgoing numbers dialed by a single telephone customer. 14

C. Location data for telephone users did not exist in the 1970s. 17

D. The Court recognized in *Riley* that modern communications services store a wealth of sensitive personal data. 24

II. Cell phone users do not "assume the risk" that their personal data will be disclosed to others. 26

A. Cell phone users expect that their personal data will be kept private. 27

B. Cell phone users limit access to their location data 31

III. This Court must determine the appropriate scope of the Fourth Amendment. Then it is for Congress to develop an appropriate statutory framework. 35

CONCLUSION 40

TABLE OF AUTHORITIES

CASES

Arizona v. Evans,
514 U.S. 1 (1995) (O'Connor, J., concurring) 23

Berger v. New York,
388 U.S. 41 (1967) 36

In re iPhone Application Litigation,
6 F. Supp. 3d 1004 (N.D. Cal. 2013) 33

Katz v. United States,
389 U.S. 347 (1967) 36

Katz v. United States,
389 U.S. 347 (1967) (Harlan, J., concurring) 36

Kyllo v. United States,
533 U.S. 27 (2001) 23, 24

Marbury v. Madison,
5 U.S. 137 (1803) 39

Riley v. California,
134 S. Ct. 2473 (2014) 6, 7, 24, 25, 26, 36, 38

Smith v. Maryland,
442 U.S. 735 (1979) 2, 6, 14, 15, 22, 27

Smith v. Maryland,
442 U.S. 735 (1979) (Marshall, J., dissenting) . 9, 27

Smith v. Maryland,
442 U.S. 735 (1979) (Stewart, J., dissenting) 8

United States v. Barajas,
710 F.3d 1102 (10th Cir. 2013) 20, 22

United States v. Caplan,
255 F. Supp. 805 (E.D. Mich. 1966) 16

United States v. Denson,
775 F.3d 1214 (10th Cir. 2014) 24

United States v. Focarile,
340 F. Supp. 1033 (D. Md. 1972) 15, 16

United States v. Giordano,
416 U.S. 505 (1974) 15

United States v. Giordano,
416 U.S. 505 (1974) (Powell, J., dissenting)..... 15

United States v. Jones,
565 U.S. 400 (2012) 9

United States v. Jones,
565 U.S. 400 (2012) (Alito, J., concurring).... 7, 9, 35

United States v. Jones,
565 U.S. 400 (2012) (Sotomayor, J.,
concurring)..... 9

United States v. Miller,
425 U.S. 435 (1976) 26

United States v. N.Y. Tel. Co.,
434 U.S. 159 (1977) 14, 15

United States v. U.S. Dist. Court for Eastern Dist. of Mich.,
407 U.S. 297 (1972) 37

United States v. Wallace, __ F.3d ___,
2017 WL 3304087 (5th Cir. 2017)..... 20

STATUTES

47 U.S.C. § 222..... 22

Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–10) 10

47 U.S.C. § 1002(a)(2)(B) 10

Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 *et seq.*) 37

50 U.S.C. § 1803 38

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–20) 37

REGULATIONS

47 C.F.R. § 20.18 21

OTHER AUTHORITIES

A Guide to the Wireless Engineering Body of Knowledge (Andrzej Jajszcyk ed., 2d ed. 2011) 18

Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83 (2014) 14

Alisdair Allan & Peter Warden, *Got an iPhone or 3G iPad? Apple is Recording Your Moves*, O'Reilly Radar (Apr. 20, 2011) 32

Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* (3d ed. 2016) 9

Apple, *About Location Services and Privacy*, Apple Support (June 21, 2017) 31

Bruce Schneier, *Data and Goliath* (2015) 23

C.F. Ault, J.H. Brewster, T.S. Greenwood, R.E. Haglund, W.A. Read, & M.W. Rolund, *IA Processor: Memory Systems*, 56 Bell Sys. Tech. J. 181 (1977) 14

Caitlin D. Cottrill & Piyushimita "Vonu" Thakuriah, *Location Privacy Preferences: A Survey-based Analysis of Consumer Awareness, Trade-off and Decision-making*, 56 Transp. Res. Part C 132 (2015) 30

Dave McHoul, *Locating a 911 Caller*, Skyhook (June 2, 2016) 21, 22

David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62 (2013) 35

Eben Moglen, *The Tangled Web We Have Woven*, 56 Comms. ACM 20 (2013) 26

EPIC, *iPhones, iPads Collect and Store User Location Data* (Apr. 21, 2011) 32

Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485 (2013) 35

G.V. King, *Centralized Automatic Message Accounting System*, 33 Bell Sys. Tech. J. 1331 (1954) 12, 13

H.R. Rep. 103-821, pt. 1 (1994) 10

Hal Abelson, Hen Ledeen, & Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (2008) 25

Hannah Arendt, *The Origins of Totalitarianism* (1973) 20

Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008) 22

Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 13, 2011, at A31 23

Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PewResearch Center (Mar. 22, 2017) 29

Kenneth Olmstead, *A Third of Americans Live in a Household with Three or More Smartphones*, PewResearch Center (May 25, 2017) 28

Laura Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 553 (2017) 19

Lee Rainie, *The State of Privacy in Post-Snowden America*, PewResearch Center (Sept. 21, 2016) 29, 30

Letter from Sen. Al Franken to Steve Jobs, CEO of Apple (Apr. 20, 2011) 33

Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, Hum. Rts., March 2013 ..... 35, 36, 37

Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013) 18

Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* (2010) 18, 19

Miguel Helft, *Jobs Said Apple Made Mistake with iPhone Data*, N.Y. Times, Apr. 27, 2011, at B3 33

Mobile Fact Sheet, PewResearch Center (Jan. 12, 2017) 28

Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce, 103d Cong. (1994) (testimony of Hon. Louis J. Freeh, Director, Fed. Bureau of Investigation) 10

Phil Lapsley, *Exploding The Phone – Extras* (2013) 13

Press Release, Apple Q&A on Location Data (Apr. 27, 2011) 34

Press Release, Markey to Apple: Is It iPhone or iTrack? (April 21, 2011) 33

Robert Ellis Smith, *Location Location Location* (2014) 22

Robert G. Harris, *State Regulatory Policies and the Telecommunications/Information Infrastructure in The Changing Nature of Telecommunications/Information Infrastructure* (Computer Sci. & Telecomm. Bd. and Nat'l Research Council eds., 1995) 14

Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2* (2003)..... 13

S. Rep. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112 37

S. Rep. No. 95-604, pt. 1 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904 38

Samuel Alito et al., Final Report, *in Conference on the Boundaries of Privacy in American Society* (1972) 38

Statement for the Record from EPIC, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties, of the House Comm. on Judiciary (June 24, 2010) 32

Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. 117 (2012) 19

Stephen J. Blumberg & Julian V. Luke, Nat. Cent. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* (2017) 28

Washington Journal: Cell Phone Tracking and Privacy Issues (C-SPAN Apr. 26, 2011) 34

Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, 30 FCC Rcd 1259 (2015) 21

Wireless E911 Location Accuracy Requirements, *Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd 2374 (2014) 21

Your Phone Dial Computes Your Bill, Popular Sci., Feb. 1949 12

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC)[1] is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts concerning privacy issues, new technologies, and constitutional interests. *See, e.g.*, *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); *Utah v. Streiff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that it is unreasonable to warrantlessly search a cell phone incident to an arrest); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (arguing that the government bears the burden of establishing the reliability of new investigative techniques used in establishing probable cause for a search); *United States v. Jones*, 565 U.S. 400 (2012) (arguing that a warrant is required for the use of GPS tracking techniques); *State v. Earls*, 214 N.J.

---

[1] Both parties have filed letters of consent to the filing of all amicus briefs with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

564 (2013) (arguing that warrantless cell phone location tracking violates the Fourth Amendment); *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (arguing that warrantless GPS tracking of a vehicle violates the Fourth Amendment).

EPIC seeks to preserve the Fourth Amendment and to prevent emerging technologies and new police practices from eroding constitutional privacy rights. This case presents a fundamental question about the scope of Fourth Amendment protections as applied to the collection of personal data—data that did not exist at the time the Court decided *Smith v. Maryland*, 442 U.S. 735 (1979). EPIC submits the following *amicus* brief, signed by distinguished technical experts and legal scholars, in support of the Fourth Amendment in the digital age.

Technical Experts and Legal Scholars

Ann M. Bartow
Director, Franklin Pierce Center for Intellectual Property and Professor of Law, University of New Hampshire School of Law

Colin J. Bennett
Professor, University of Victoria

Francesca Bignami
Professor of Law, The George Washington University Law School

David Chaum
Chaum, LLC

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, University of Maryland School of Law

Julie Cohen
Mark Claster Mamolen Professor of Law and Technology, Georgetown Law

Jennifer Daskal
Associate Professor, American University Washington College of Law

Dr. Whitfield Diffie

Laura K. Donohue
Professor of Law, Director of The Center for National Security and the Law, Georgetown University Law Center

Cynthia Dwork
Distinguished Scientist, Microsoft Research

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

Deborah Hurley
Harvard University and Brown University

Ian Kerr
Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Chris Larsen
Executive Chairman, Ripple, Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya,
Professor of Computer Science, Brown University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
Library Law Consultant

Erin Murphy
Professor of Law, NYU School of Law

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science, Professor, New York University (on leave), Media, Culture, and Communication & Computer Science

Dr. Deborah Peel, M.D.
Founder and Chair, Patient Privacy Rights

Ronald L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law and Information, University of California, Berkeley School of Law; Co-Director, Berkeley Center for Law & Technology

Bruce Schneier
Program Fellow, Harvard Kennedy School

Robert Ellis Smith
Publisher, Privacy Journal

Dr. Barbara Simons,
IBM Research (retired)

Nadine Strossen
John Marshall Harlan II Professor of Law, New York Law School; Former President, American Civil Liberties Union

Sherry Turkle,
Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, MIT

Edward G. Viltz,
President and Chairman, Internet Collaboration Coalition

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, Chief Technology Officer, John A. Paulson School of Engineering and Applied Science, Professor of Technology Policy, Harvard Kennedy School

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff,
Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Smith v. Maryland, 442 U.S. 735 (1979), arose in a world that no longer exists. In the 1970s, telephones were tethered to homes, offices, and street corners. Cell phones were not available, and logs of telephone customers' locations over the course of a day were neither recorded nor available for later inspection. Cell phones are now as necessary to the life of Americans as they are ubiquitous. They are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of the human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). Yet, despite these fundamental changes, lower courts still apply Fourth Amendment concepts that were established when rotary phones sat on desk tops, the receivers connected with coiled wire.

This Court has never held that the government may search and seize records of where a person travels without triggering Fourth Amendment scrutiny. Indeed, the Court recently determined in *Riley* that the government could not seize such sensitive cell phone data without a warrant. There is also no evidence that cell phone users expect to be subject to such routine tracking of their private lives– quite the contrary. We as a society are not prepared to accept pervasive, warrantless location tracking as objectively reasonable.

The Court's decision in *Smith* does not determine the scope of Fourth Amendment protection today. In the modern era, cell phone location records provide a "comprehensive record of a person's public movements that reflects a wealth of detail about her

familial, political, professional, religious, and sexual associations." *Riley*, 134 S. Ct. at 2490 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). And while Congress should address the "complex subject" of location tracking by enacting a "comprehensive statute," the Court bears the fundamental responsibility of determining the appropriate scope of the Fourth Amendment. *See Jones*, 565 U.S. at 427 (Alito, J., concurring); *see also* Edith J. Lapidus, *Eavesdropping on Trial* 1–26 (1974) (discussing the development of modern wiretap law, particularly the importance of the Court's decisions in *Berger* and *Katz* in the 1967 term that led to adoption of a comprehensive privacy law in 1968).

ARGUMENT

This case involves the warrantless collection of cell phone location records. In 1979, that data did not exist. Today, that data is maintained on all cell phone users in the United States. If the warrantless collection of location data is permissible in this case, then it would be permissible for every cell phone customer in the country.

In *Jones* (2012), this Court held unanimously that the warrantless tracking of a person's movement by means of a GPS attached to a vehicle was impermissible. Then the Court held in *Riley* (2014) that the traditional "search incident to arrest" exception did not apply to cell phones, given the wealth of personal data stored on the devices.

Despite the Court's recent rulings and the fundamental shift in communications technology that

has occurred since the 1970s, lower courts continue to follow *Smith* (1979) and hold that the Fourth Amendment does not apply to cell phone location data. These decisions are out of step with the current era. First, *Smith* is no longer applicable in the age of cell phones; modern call data bears little resemblance to the paper logs available in 1979. Second, cell phone users do not "assume the risk" that their personal data will be made available to any person at any time. Third, it is the Court and not Congress that should determine the appropriate scope of Fourth Amendment protections.

Even at the time that *Smith* was decided, the Court was closely divided over the appropriate degree of protection for pen register information. Justice Stewart was sharply critical of the Court's conclusion, noting that:

> I think that the numbers dialed from a private telephone--like the conversations that occur during a call--are within the constitutional protection recognized in *Katz*. It seems clear to me that information obtained by pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy.

Smith, 442 U.S. at 747 (Stewart, J., dissenting). Justice Marshall also dissented, challenging the Court's "assumption of risk" analysis:

> [E]ven assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a

> discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes . . . .

Smith, 442 U.S. at 749 (Marshall, J., dissenting).

Since *Smith* was decided in 1979, both the Court and Congress have recognized the need to limit warrantless location tracking. The Court unanimously rejected the government's argument in *Jones* that the attachment and use of a GPS device to track an individual's movements over several months was not a search under the Fourth Amendment. *Jones*, 565 U.S. 400. Five members of the Court agreed with Justice Alito's conclusion that "the lengthy monitoring that occurred . . . constituted a search under the Fourth Amendment." *Jones*, 565 U.S. at 431 (Alito, J., concurring); *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"); Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* 443 (3d ed. 2016) (explaining the view that "there were five votes [in *Jones*] for a *Katz*-based determination that GPS tracking violates the Fourth Amendment"). The Court's majority opinion in *Jones* also recognized that modern location tracking techniques make possible "dragnet-type law enforcement practices" that the Court explicitly refused to authorize in the 1980s beeper cases. *Jones*, 565 U.S. at 409 n.6 (quoting *United States v. Knotts*, 460 U.S. 276, 284 (1983)).

Congress has also recognized that special protections for location data are necessary to protect expectations of privacy. In 1994 Congress passed the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–10), at the behest of then-FBI Director Louis Freeh. But even as Congress was significantly expanding law enforcement surveillance powers in CALEA, it explicitly prohibited the government from obtaining "any information that may disclose the physical location of the subscriber" when acting "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2)(B). Congress recognized that, at the time, "some cellular systems" generated "transactional data that could be obtained by a pen register [which] may include location information." H.R. Rep. No. 103-821, pt. 1, at 17 (1994). This limitation was proposed by the FBI as an assurance that the agency was not seeking a "pervasive, automated 'tracking' capability." *Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 54 (1994) (testimony of Hon. Louis J. Freeh, Dir., Fed. Bureau of Investigation). Yet now the Government argues that the same location data it encouraged Congress to protect in 1994 should not be protected under the Fourth Amendment.

I. The world has changed since *Smith v. Maryland*. The widespread use of mobile phones and the routine collection of detailed location data was not possible in 1979.

The analog telephone network of the 1970s was entirely unlike today's digital network. In 1979, when *Smith* was decided, telephone service was provided as a public utility, local calls were not individually billed, and there was little transactional data generated by a private communication. It was only after the transition to "Signal System 7" ("SS7"), which followed *Smith*, that the challenge of collecting, storing, analyzing, safeguarding, and securing digital phone records emerged. In 1979, no one could have used call detail records to trace an individual's movements over time. A telephone number was tied to an address, not to an individual. Many phones were shared by multiple users in a home or office. In short, the records at issue in *Smith* revealed the numbers dialed, not a person's location. Today the communications network provides a vast range of voice, data, and messaging services and simultaneously records every transaction that occurs, tied directly to particular subscribers.

A. The analog phone system in the 1970s did not generate "out of band" personal data.

In the period leading up to the Court's decision in *Smith*, detailed phone records simply did not exist for local calls. Prior to the introduction of the earliest electronic switching systems in the 1960s and 1970s, the majority of telephone calls in the United States

were processed by analog switches that had limited accounting and billing capabilities. These analog switches relied on "Automatic Message Accounting" systems, which were introduced in the Bell System in 1948 and recorded customer data on perforated paper tapes (earlier systems relied on handwritten notes from telephone operators). G.V. King, *Centralized Automatic Message Accounting System*, 33 Bell Sys. Tech. J. 1331, 1332 (1954). These analog accounting systems were designed to handle three different types of calls: flat-rate local calls, message rate calls, and long distance toll calls. *Your Phone Dial Computes Your Bill*, Popular Sci., Feb. 1949, at 135–36. Most local calls were billed on a flat-rate monthly basis, and automated accounting equipment was not used to record any details about these calls. King, *supra*, at 1333. For calls billed on a message rate basis, the accounting system would record a two-line entry containing "the calling office code and telephone number, the billing index and the trunk identity," along with the duration of the call. *Id.* at 1339. The more extensive four-line entries also contained "the called office code and telephone number" but were only used for detail-billed toll calls and special bulk billed calls that required additional records. *Id.* In situations where a toll call could not be completed by a switch capable of automated message accounting, customers had to be connected via an operator who would manually record the details of each call. *Id.* at 1334–35.

As the automatic message accounting system was deployed throughout the United States beginning in the 1950s, it was necessary to centralize the accounting function due to the high cost of the infrastructure relative to the volume of toll calls at many

of the smaller local telephone offices. King, *supra*, at 1333; *see also* Phil Lapsley, *Exploding The Phone – Extras* (2013).[2] The automated message accounting system also evolved with the development of "automatic number identification" technology, which was deployed to ensure billing accuracy throughout the Bell System by 1961. *See* Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 35 (2003). During the 1950s and 1960s, the Bell System continued to install and use centralized automatic message accounting systems, *see* Lapsley, *supra*, while Bell Laboratories conducted research into new electronic switching systems. Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 48–56 (2003). The integration of digital computing technology into the telecommunications industry was ongoing throughout the 1970s, and the evolution of telecommunications services was rapid. *See id.* at 114–15. The first electronic switching system, No. 1 ESS, developed by Western Electric and Bell Laboratories, was put into operation in Succasunna, New Jersey in 1965. Each of the 24 Regional Bell Operating Companies had installed at least one ESS by 1967. *Id.* at 158. These electronic switching systems began using magnetic tape drives to store call detail information in the 1970s, but memory was limited and the storage of call details was necessarily temporary. *See id.* at 345.

In the 1970s there were no detailed records for most calls. Local call records were ephemeral because most customers paid a flat monthly rate and did not receive itemized bills. Robert G. Harris, *State Regula-*

---

[2] http://explodingthephone.com/extras/ama.php.

tory Policies and the Telecommunications/ Information Infrastructure in The Changing Nature of Telecommunications/Information Infrastructure (Computer Sci. & Telecomm. Bd. and Nat'l Research Council eds., 1995).

Even after the development of advanced electronic switching technologies, telephone companies had little incentive to store transactional data. By the mid-1970s, magnetic tape backup storage was integrated into the most advanced electronic switches. C.F. Ault, J.H. Brewster, T.S. Greenwood, R.E. Haglund, W.A. Read, & M.W. Rolund, *1A Processor: Memory Systems*, 56 Bell Sys. Tech. J. 181, 201 (1977). But there was little space to store phone records as bandwidth had to be preserved for other functions. That all changed after cell phone use became widespread and the government began requiring all wireless carriers to build increasingly accurate location tracking systems.

B. The pen register in *Smith* recorded only the outgoing numbers dialed by a single telephone customer.

Even the Court in *Smith* recognized that the pen registers had "limited capabilities." 442 U.S. at 741; *see also* Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 101–05 (2014). The records in *Smith* did not reveal whether a call had been completed or whether any conversation took place. The Court in *Smith* relied on the definition of a pen register established in two earlier cases, which also emphasized the limited tracking ability of the device: *United States v. New York Telephone Company*, 434 U.S. 159 (1977), and

United States v. Giordano, 416 U.S. 505 (1974). *See Smith*, 442 U.S. at 736 n.1.

In these prior cases, the Court relied on the limited capability of a pen register in determining the application of the Wiretap Act. In *New York Telephone*, the Court rejected a phone company's challenge to an FBI pen register order. 434 U.S. at 165–66. The Court found that use of a pen register did not result in an "interception" of communications, and would "disclose only the telephone numbers that have been dialed." *Id.* at 167. In *New York Telephone*, the Court emphasized that "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.*

Earlier, in *United States v. Giordano*, 416 U.S. 505 (1974), Justice Powell, writing for four members of the Court in dissent, also emphasized the limited capabilities of a pen register. The dissent argued that evidence collected by a pen register should not be suppressed because the device was "not governed by Title III." *Id.* at 553–54 (Powell, J., dissenting). Justice Powell stressed that the device "did not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed." *Id.* at 549 n.1.

Justice Powell's description of a pen register, which was relied upon by the Court in *Smith*, was based on the description of lower court in *Giordano*. *Id.* The lower court had found that a pen register was nothing more than a "decoder" used to translate electric tones generated during a phone's dialing operation. *United States v. Focarile*, 340 F. Supp. 1033, 1039 40 (D. Md. 1972). The rotary phone at issue in

Giordano signaled the numbers dialed when "a switch opened and closed a corresponding number of times to the digit dialed which in turn interrupt[ed] the direct current on the line and cause[d] the voltage of the electrical current to rise or fall the corresponding number of times." *Id.* at 1039. The pen register device, once installed on the phone line, would count "the number of pulses in the electrical energy caused by the changes in voltage, and cause[] the digit dialed on the telephone to be printed in Arabic numerals corresponding to the number of electric pulses." *Id.* A similar record could be generated for touch tone phone calls, though it required a more sophisticated technique. *Id.* at 1040.

Other courts reviewing pen register evidence during that period produced similar findings: pen registers only collected limited details about outgoing calls. *See, e.g., United States v. Caplan*, 255 F. Supp. 805, 807 (E.D. Mich. 1966) ("With reference to incoming calls, the pen register records only a dash for each ring of the telephone but does not identify the number from which the incoming call originated. The pen register cuts off after the number is dialed on outgoing calls and after the ringing is concluded on incoming calls without determining whether the call is completed or the receiver is answered.").

In 1979, when *Smith* was decided, a pen register log would show nothing more than the fact that a call was made at a specific time (e.g. 12:34 PM) to a specific number (e.g. 555-555-5555).

C. Location data for telephone users did not exist in the 1970s.

The contrast between the limited pen register records at issue in *Smith* and the cell phone location data in this case could not be more pronounced. A pen register in the 1970s could only record the number dialed by a target phone and the time the call was made. Most phones were not associated with an individual person, and a pen register could not even show whether any communication took place. Modern cell phone records include an entirely different category of information – location data—that can be used to map an individual's movements over time. That is precisely what happened in this case. The availability of increasingly precise location data underscores the need for a clear Fourth Amendment standard protecting against warrantless location tracking.

The privacy implications of cell phones arise from the structure of wireless communications networks. Unlike landline phones, cell phones generate precise location data that can be used to track an individual's movements over time. A cell phone is "a very sophisticated and versatile" device that uses radio waves to send and receive voice calls and data whenever it is within range of an antenna or tower. CTIA: The Wireless Association, *Wireless in America: How Wireless Works.*[3] Cell phones connect to a service provider's network via "cell sites," each of which contains a transceiver and controller used to relay signals between mobile devices and the network to enable calls and other communications. Axel Küpper,

---

[3] http://files.ctia.org/pdf/Brochure_HowWirelessWorks.pdf.

Location-Based Services: Fundamentals and Operation 91–97 (2006). *See generally* CDG, *Welcome to the World of CDMA: Glossary* (1999);[4] Tom Farley & Mark van der Hoek, *Cellular Telephone Basics* (2004).[5]

The data created when a cell phone communicates with a tower can be used to determine the location of the device and, in turn, the location of the person using the phone. Mobile devices communicate with nearby cell sites during a process called "registration," which occurs automatically even when the device is idle. *A Guide to the Wireless Engineering Body of Knowledge* 77 (Andrzej Jajszcyk ed., 2d ed. 2011). During the registration process, mobile devices ping nearby cell sites to identify the strongest signal. Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* 104 (2010).

A similar process occurs when a user moves from one cell site to another while making a call. Once registration occurs, the information is stored temporarily in service provider databases in order to route calls. Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013).[6] Typically a log is created every time a call is made or data downloaded, *see* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location*

---

[4] http://www.cdg.org/technology/cdma_technology/a_ross/DefAtoF.asp.

[5] *Available at* https://web.archive.org/web/20041128222046/http://www.privateline.com:80/cellbasics/Cellbasics.pdf.

[6] http://www.crypto.com/blog/celltapping/.

Data that Congress Could Enact, 26 Berkeley Tech. L.J. 117, 128 (2012), including when smart phone apps access the internet without a user's knowledge. Sequeira & Westphal, *supra*.

Law enforcement investigators use this data to pinpoint the locations of people they are tracking. As Professor Laura Donohue has explained, "[s]ervice providers record where users' mobile devices connect to local towers— and not just when a telephone call is made or a text message is received, but constantly, as the user moves through space. The information provides a picture of where individuals go." Laura Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 553, 618–19 (2017). Maps can be created and introduced as evidence. In this case, the United States submitted maps and a report from the FBI's "Cellular Analysis Survey Team." *See* SA Christopher J. Hess, Detroit Division, Detroit Major Crimes Task Force, *Cellular Analysis* (Nov. 5, 2013), ECF No. 211-2.

Location data can precisely locate an individual because (1) cell phones "constantly scan their environment looking for the best signal," and (2) "the best signal generally comes from the tower that is CLOSEST to the phone, or is in direct LINE OF SIGHT." *Id.* at 5. The records show which cell site the target was connected to when each call was initiated and when each call ended. *Id.*

These cell site records reveal more than whether a user was somewhere near a tower. Cell towers typically have three 120° "sectors," and the antennas "have a downwards tilt" such that each sector covers the area of "an upside-down funnel." *Id.* 5–6. By comparing the cell site records with tower loca-

tion and sector data, law enforcement can generate precise location data that can be visualized using computer mapping software. *See, e.g., id.* at 11–15.[7]

Cell site location information is not the only type of location data that has been seized in criminal cases. In addition to historical cell site location information, officers often seize cell site and GPS data in real time. *See, e.g., United States v. Wallace*, ___ F.3d ___, 2017 WL 3304087 (5th Cir. 2017) (officer used a "Ping Order" to "obtain real-time geolocation coordinates"); *United States v. Barajas*, 710 F.3d 1102 (10th Cir. 2013) (DEA agent obtained from the cell phone provider "GPS coordinates for the location of [the] telephone within a certain radius" in real time).

Cell phone providers have developed real-time location tracking methods to comply with regulations

---

[7] Hannah Arendt warned that such capability would enable the emergence of a totalitarian state:

> Now the police dreams that one look at the gigantic map on the office wall should suffice at any given moment to establish who is related to whom and in what degree of intimacy; and, theoretically, this dream is not unrealizable although its technical execution is bound to be somewhat difficult. If this map really did exist, not even memory would stand in the way of the totalitarian claim to domination; such a map might make it possible to obliterate people without any traces, as if they had never existed at all.

Hannah Arendt, *The Origins of Totalitarianism* 434 (1973).

that require providers to be able to locate a 911 caller in an emergency. *See* 47 C.F.R. § 20.18. The FCC has increased the location accuracy requirements in the decades since they were first introduced as users have transitioned from land lines to mobile phones. Wireless E911 Location Accuracy Requirements, *Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd 2374 ¶1 (2014) ("[T]oday, the majority of 911 calls come from wireless phones."). The FCC now requires that providers be able to accurately locate users indoors. Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, 30 FCC Rcd 1259 ¶ 1, 6 (2015). All providers must have the capability to pinpoint a 911 caller within 50 meters horizontally and develop a method for establishing vertical ("z-axis") location data as well. *Id.* ¶ 6.

Providers currently use triangulation (or "lateration") methods based on the simultaneous signals received by different base stations. *See* Ali H. Sayed, Alireza Tarighat & Nima Khajehnouri, *Network-Based Wireless Location*, IEEE Signal Processing Magazine 24, 26–29 (Jul. 2005); *see also* Axel Küpper, *Location-Based Services: Fundamentals and Operation* 131–36 (2006). An even more precise location record can be calculated using the exact angle and time of arrival of each signal. *See id.* at 138–40, 144–48. One example of such a system is the U-TDOA technique implemented by Skyhook and used by current mobile carriers. Dave McHoul, *Locating a 911 Caller*, Skyhook (June 2, 2016).[8] In response to the FCC's "indoor mandate," providers are deploying new

[8] http://blog.skyhookwireless.com/precision/location/locating-a-911-caller.

techniques that can locate a device even when the call is placed indoors. *Id.* "[T]he line between public and private modes of surveillance and security has blurred if not vanished." Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 7 (2008).

The use and disclosure of emergency call data is restricted under the Federal Communications Act, which mandates that service providers protect consumer privacy by limiting disclosure of consumer proprietary network information ("CPNI"). *See* 47 U.S.C. § 222.[9] Despite the fact that the E-911 system was developed to be used for emergencies, law enforcement has demanded access to the same data for criminal enforcement purposes. *See, e.g.*, *Barajas*, 710 F.3d at 1104 n.1.

Although the Court observed in *Smith* that "[n]umbers dialed to and from a phone are not entitled to as much privacy protection as the content of the conversation," *Smith*, 442 U.S. at 735, "[i]n 2014 the opposite is true. Most cell conversations are not probative, not sensitive, not revealing. But the numbers dialed to us and from us show our associations and our patterns." Robert Ellis Smith, *Location Location Location* 3 (2014). Indeed, as computer security expert Bruce Schneier has explained, "location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone

---

[9] There are only three exceptions to the CPNI rule that allow disclosure of cell phone location information: (1) to an emergency 911 service, (2) to inform a legal guardian in an emergency, and (3) to assist in the delivery of emergency services. 47 U.S.C. § 222(d)(4).

willing to pay for it." Bruce Schneier, *Data and Goliath* 2 (2015).[10] National Constitution Center President Jeffrey Rosen, writing about similar issues before the Court in *Jones*, and acknowledging the views of Judge Douglas Ginsberg, warned that "[i]f the court rejects his logic and sides with those who maintain that we have no expectation of privacy in our public movements, surveillance is likely to expand, radically transforming our experience of both public and virtual spaces." Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 13, 2011, at A31.

Justice O'Connor has also emphasized the need to maintain constitutional safeguards as new technologies emerge. "With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring). And as Justice Scalia explained for the Court in *Kyllo v. United States*:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

533 U.S. 27, 33–34 (2001).

Justice Scalia concluded in *Kyllo* that the use of a thermal imaging device to record activities inside the home would "permit police technology to erode the privacy guaranteed by the Fourth Amendment,"

---

[10] http://www.educause.edu/ir/library/pdf/LIVE1402.pdf.

and must therefore be considered a search. *Id.* at 34. "This assures," as Justice Scalia explained, "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.*; *see also United States v. Denson*, 775 F.3d 1214 (10th Cir. 2014) ("New technologies bring with them not only new opportunities for law enforcement to catch criminals but also new risks for abuse and new ways to invade constitutional rights.").

D. The Court recognized in *Riley* that modern communications services store a wealth of sensitive personal data.

Location information is just one element in the constellation of sensitive data that cell phone users regularly entrust to service providers. As the Court explained in *Riley*, modern cell phones are used to create, receive, and access a "broad array of private information," *Riley*, 134 S. Ct. at 2491:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. . . . . Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. . . . Data on a cell phone can also reveal where a person has been. Historic location information is

> a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Id. at 134 S. Ct. at 2489–90. Moreover, much of the private data created and accessed with cell phones is actually stored on remote servers:

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. . . . Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.

Id. (citing Brief for Electronic Privacy Information Center at 12–14, 20, *Riley*, 134 S. Ct. 2473 (No. 13–132)). "So much digital information, misinformation, data, and garbage is being squirreled away . . . . And computers are getting better and better at extracting meaning . . . sometimes reveal[ing] things about us we did not expect others to know." Hal Abelson, Hen Ledeen, & Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* 2 (2008). "[W]e are rapidly adopting personal service robots . . . . They see what we point them at; they have ears to hear everything going on around us; they know our location all the time. These robots we call smartphones and tablets often contain software we cannot read or understand, much less change."

Eben Moglen, *The Tangled Web We Have Woven*, 56 Comms. ACM 20, 21 (2013).

Given the sensitive nature of the cell phone data that is stored remotely and this Court's requirement that the Government obtain a warrant before conducting a search of a phone, *Riley*, 134 S. Ct. at 2495, it would be illogical to hold that the same data, once uploaded to a remote server, is no longer protected. Yet that is the sweeping implication of the Government's argument that it can collect cell phone location data without a warrant. Sensitive personal data—photos, emails, location information, or otherwise—does not become less private simply because a cell phone user entrusts that information to a communications service provider.

II. Cell phone users do not "assume the risk" that their personal data will be disclosed to others.

Extending the concept of "assumption of risk," relied upon by the Court in *Smith*, to cell site location information would ignore technological changes and defy common sense.

In *Miller*, the Supreme Court concluded that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 443 (1976). In *Smith*, the Court extended this logic to call detail records based on a finding that the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business . . . assum[ing] the risk that

the company would reveal to police the numbers he dialed." *Smith*, 442 U.S. at 744.

Yet this "assumption of risk" construct does not apply to the modern cell phone user. Consumers do not assume the risk that their personal data will be disclosed by their cell phone providers simply because of their participation in an essential part of modern life. In the reality, cell phone users now make exactly the opposite assumption. Survey data demonstrates that individuals expect their personal data to be kept private by their service providers.

A. Cell phone users expect that their personal data will be kept private.

Particularly important for the case before this Court, mobile phone users today are concerned about the collection and use of their location data. In *Smith*, Justice Marshall wrote in dissent that "unless a person is prepared to forgo" the telephone, for "many . . . a personal or professional necessity, he cannot help but accept the risk of surveillance." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting). He concluded that "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.*

This warning has proved prescient. Cell phones are an essential part of modern life. Americans use them for purposes ranging from the intimate to the mundane; the devices are often in our pockets, purses, or backpacks everywhere we travel—from church, to school, to home, to the political rally, and the doctor's office. In opinion surveys, Americans express deep concerns about data privacy, skepticism

about companies' business practices, and a desire for limits on location data tracking.

Americans rely on cell phones to participate in life. 95% of Americans own a cell phone. *Mobile Fact Sheet*, PewResearch Center (Jan. 12, 2017).[11] That number rises to 100% for 18- to 29-year-olds. *Id.* 84% of American households have at least one smart phone, and a third have three or more. Kenneth Olmstead, *A Third of Americans Live in a Household with Three or More Smartphones*, PewResearch Center (May 25, 2017).[12] Phones are also the sole source of internet access at home for one in ten Americans, a trend that is even stronger among younger, non-white, and lower-income Americans. *Mobile Fact Sheet*, PewResearch Center (Jan. 12, 2017).[13] A recent study shows that now "a majority of American homes ha[ve] only wireless telephones." Stephen J. Blumberg & Julian V. Luke, Nat. Cent. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* at 1 (2017).

A 2016 PewResearch survey documents that Americans are deeply concerned about privacy. Pew discovered that "65% of Americans say there are not adequate limits on 'what telephone and internet data the government can collect.'" Lee Rainie, *The State of Privacy in Post-Snowden America*, PewResearch Cen-

---

[11] http://www.pewinternet.org/fact-sheet/mobile/.

[12] http://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/.

[13] http://www.pewinternet.org/fact-sheet/mobile/.

ter (Sept. 21, 2016).[14] Pew also found that individuals are trying to protect their privacy: "86% of Internet users have taken steps online to remove or mask their digital footprints." *Id.* A majority of users (61%) say they would like to do more to protect their personal information online. *Id.* Users certainly do not consent to location tracking; only 52% of those surveyed understood "that turning off the GPS function of a smartphone *does not* prevent all tracking of that device." Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PewResearch Center (Mar. 22, 2017).[15]

According to the Pew survey, a clear majority of Americans say that it is "very important" to be "in control of who can get information about them" and "to control what information is collected about them." Rainie, *supra*. Yet Americans also "express a consistent lack of confidence" that that "records will remain private and secure," and 56% are either not too confident or not at all confident that cell phone companies adequately protect their records. *Id.*

Young adults between 18 and 29 "generally are more focused than their elders when it comes to online privacy." *Id.* And while "younger adults are more likely to have shared personal information," that does not negate their privacy concerns. *Id.* In fact, the opposite is true. This group is most likely to "have paid attention to privacy issues." *Id.* Similarly, they are more likely to have taken active steps to pro-

---

[14] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[15] http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

tect their privacy such as "limit[ing] the amount of personal information available about them online, chang[ing] privacy settings, delet[ing] unwanted comments on social media, remov[ing] their name from photos in which they were tagged, and tak[ing] steps to mask their identities while online." *Id.*

Many users say that their privacy is at risk when location or travel data is gathered by a third party. Those numbers increase to substantial majorities when that data is later shared with law enforcement agencies without a warrant. In one survey, for instance, 51% of respondents indicated they either agreed or strongly agreed that having "location or travel data collected and stored by a private company (such as Google)" placed their privacy at risk. Caitlin D. Cottrill & Piyushimita "Vonu" Thakuriah, *Location Privacy Preferences: A Survey-based Analysis of Consumer Awareness, Trade-off and Decision-making*, 56 Transp. Res. Part C 132 (2015). Over 71% of respondents either agreed or strongly agreed that their privacy would be placed at risk by "[h]aving location or travel information gathered by a private company . . . shared with law enforcement agencies with no warrant issued" as the government seeks to do here. *Id.*

In short, the privacy interests of Americans have not diminished with the widespread use of cell phones. Instead, consumers express concern and seek to protect their personal data. Far from "assuming the risk" associated the new technology, cell phone users reasonably expect that the records of their activities will be protected.

B. Cell phone users limit access to their location data.

At the time *Smith* was decided, there was no extrinsic evidence about individual users' expectations regarding the privacy of the numbers dialed; users had no choice if they wanted to make a call. But in the era of smart phones, users have a wide range of tools and settings available to enhance the privacy of their cell phone data. Responding to demand, mobile companies and apps are increasing the availability of location privacy controls. Today, these controls are basic privacy features of all major cell phone models and mobile applications. The availability of location settings demonstrates that individuals are not, in any meaningful way, "assuming the risk" that their location data will be revealed by service providers. Instead, users are taking active steps to maintain privacy of their personal data.

The Apple iPhone allows users to disable location services for the device entirely. Apple, *About Location Services and Privacy*, Apple Support (June 21, 2017).[16] These safeguards in the modern cell phone follow almost directly from concerns expressed by users about location tracking.

In 2011 Apple faced pressure after two security researchers revealed Apple was routinely storing location data in hidden files on iPhones and iPads. The pair found that Apple devices running iOS 4 consistently recorded time-stamped latitude-longitude coordinates. Alisdair Allan & Peter Warden, *Got an iPh-*

---

[16] https://support.apple.com/en-us/HT207056.

one or 3G iPad? Apple is Recording Your Moves, O'Reilly Radar (Apr. 20, 2011).[17] Moreover, the data was stored in an unencrypted file called "consolidated.db," which could easily be compromised by third parties. *Id.* The data logs tracked as much as a year's worth of movements—the time between release of the operating system and the security flaw's discovery—and the data cache was transferred for backup purposes anytime the device was synced. *Id.*

EPIC had previously warned about the expansion of location tracking by Apple and other companies. *See* Statement for the Record from EPIC, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties, of the House Comm. on Judiciary (June 24, 2010).[18]

Users were outraged when they learned about this surreptitious location tracking. *See* EPIC, *iPhones, iPads Collect and Store User Location Data* (Apr. 21, 2011).[19] Representative Edward Markey wrote to Steve Jobs the next day, demanding answers to questions about the data collection. "Apple needs to safeguard the personal location information of its users to ensure that an iPhone doesn't become an iTrack." Press Release, Markey to Apple: Is It iPhone

---

[17] http://radar.oreilly.com/2011/04/apple-location-tracking.html.

[18] https://epic.org/privacy/ECPA_Statement_2010-06-24.pdf.

[19] https://epic.org/2011/04/post-10.html.

or iTrack? (April 21, 2011).[20] The Congressman pressed the company about compliance with user consent requirements of § 222 of the Communications Act. *Id.* Senator Al Franken also wrote to the CEO asking for a "prompt response" to a series of questions, including why this data was compiled in the first place and why the company failed to secure it. Letter from Sen. Al Franken to Steve Jobs, CEO of Apple (Apr. 20, 2011).[21] A class action lawsuit was filed against the company in district court alleging violations of the Computer Fraud and Abuse Act and state unfair and deceptive trade practice laws. *See In re iPhone Application Litigation*, 6 F. Supp. 3d 1004 (N.D. Cal. 2013).

In response to the public outcry, "Steven P. Jobs, Apple's chief executive, took the unusual step of personally explaining that while Apple had made mistakes in how it handled location data on its mobile devices, it had not used the iPhone and iPad to keep tabs on the whereabouts of its customers." Miguel Helft, *Jobs Said Apple Made Mistake with iPhone Data*, N.Y. Times, Apr. 27, 2011, at B3. According to the New York Times, Jobs stated, "We haven't been tracking anybody. Never have. Never will." *Id.*

Within a week, the company announced it would release a software update to address privacy and data security concerns. Press Release, Apple

---

[20] https://www.markey.senate.gov/news/press-releases/april-21-2011-markey-to-apple-is-it-iphone-or-itrack.

[21] https://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf.

Q&A on Location Data (Apr. 27, 2011).[22] The update restricted storage of location data, stop the automated transfer of location data, and completely purged all location data when a user turned off location services. *Id.* The company also announced that the next major software release would encrypt cached location data. *Id.*

As the New York Times recounted the battle: "Some privacy advocates who were harshly critical of Apple last week praised the company's response, saying it was a step in the right direction." Helft, *supra*. The Times also quoted EPIC Executive Director Marc Rotenberg as stating, "Apple acknowledged a mistake and they fixed it. . . . That's a good thing." *Id.*; *see also Washington Journal: Cell Phone Tracking and Privacy Issues* (C-SPAN Apr. 26, 2011).[23]

In sum, cell phone users today have made clear their strong belief in privacy protections, so much so that the CEO of the company that produces the most popular cell phone in the world was required to respond quickly when the company inadvertently collected location data.

---

[22] https://www.apple.com/newsroom/2011/04/27Apple-Q-A-on-Location-Data/.

[23] https://www.c-span.org/video/?299201-4/cell-phone-tracking-privacy-issues.

III. This Court must determine the appropriate scope of the Fourth Amendment. Then it is for Congress to develop an appropriate statutory framework.

The Court and Congress have long worked together to determine the scope of the right to privacy. Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, Hum. Rts., March 2013, at 7, 10. ("Both courts and Congress share responsibility for safeguarding individuals' privacy from advancing technology and overzealous government surveillance."). Congress brings the ability for detailed fact-finding and the development of clear rules set out in public law. "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 565 U.S. at 427–28 (Alito, J., concurring) (internal citations omitted); *see also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 110 (2013) ("[T]he law enforcement and privacy interests at stake can be explored in a more expansive and timely manner in the context of legislative or executive rule making processes than they can be in the context of constitutional litigation."); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485, 535 (2013) ("Congress has proven more adept than the courts at implementing mechanisms for systemic oversight of privacy

practices, as well as for reform of noncompliant institutions.").

But Congress should follow the lead of the Court as new conflicts between law enforcement practices, emerging technology, and Fourth Amendment privacy protections emerge. Rotenberg & Brody, *supra*, at 10 ("Privacy protection under the Fourth Amendment is first and foremost the responsibility of the courts."). With the Court's constitutional guidance, Congress can take its turn and enact privacy legislation "that draws reasonable distinctions based on categories of information or [] other variables." *Riley*, 134 S. Ct. at 2497.

"The regulation of electronic surveillance provides an instructive example" of Congress's complementary role in defining privacy protections. *Id.* In 1967, the Court struck down a New York statute because it permitted electronic eavesdropping "without requiring belief that any particular offense ha[d] been or [was] being committed" and without requiring that the "conversations [sought] be particularly described." *Berger v. New York*, 388 U.S. 41, 58–59 (1967). Later that term, the Court held that warrantless eavesdropping on a telephone booth violated the Fourth Amendment because it intruded on the caller's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 358–59 (1967); *id.* at 360 (Harlan, J., concurring).

It was only after the landmark *Berger* and *Katz* decisions that Congress developed a comprehensive statutory framework governing electronic surveillance. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Tit. III, 82 Stat. 197,

211–25 (codified as amended at 18 U.S.C. §§ 2510–20). In drafting Title III, Congress expressly relied on the factors that the Court had set out in *Berger* and *Katz*. S. Rep. No. 90-1097, 73–75 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2161–63 ("Working from the hypothesis that any wiretapping and electronic surveillance legislation should include . . . constitutional standards, the subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III."). "It was the Court's decision in 1967 that set the course for the modern right to privacy, but it was the congressional legislation the following year that gave meaning to that right." Rotenberg & Brody, *supra*, at 10.

This dialogue between the Court and Congress continued into the 1970s over the issue of national security surveillance. In *United States v. U.S. Dist. Court for Eastern Dist. of Mich.*, 407 U.S. 297 (1972) (*Keith*), the Court held that the Fourth Amendment requires the government to comply with an "appropriate prior warrant procedure" before conducting surveillance for domestic security purposes. *Id.* at 320. The distinction drawn by the *Keith* Court between surveillance of foreign and domestic parties was foundational to Congress's enactment of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 *et seq.*). As the Senate Report explained, the statute would "not authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a domestic nature." S. Rep. No. 95-604, pt. 1, at 26 (1978), *as re-*

printed in 1978 U.S.C.C.A.N. 3904, 3928. Congress thus took its constitutional cues from the Court's Fourth Amendment jurisprudence.

Justice Alito, as a college student, even anticipated this development. Writing in 1972 as the *Keith* case was ongoing, Justice Alito set out the contours of federal legislation for a court of national security warrants:

> A Federal Court of Warrants should be created to issue warrants for electronic surveillance in *all* cases involving the national security. . . . Recognizing both that the usual procedures may be inappropriate in cases involving the national security and that the system proposed by the government is highly susceptible to abuses, we propose that a Federal Court of Warrants be created solely for the purpose of hearing these cases.

Samuel Alito et al., Final Report, *in Conference on the Boundaries of Privacy in American Society* 6, 10–11 (1972).[24] Within seven years, Congress had enacted the FISA and established the Foreign Intelligence Surveillance Court. 50 U.S.C. § 1803.

The Court remains the interpreter of the Fourth Amendment in our modern age. The government's practice of obtaining cell phone location data without a warrant is out of step with the Court's recent opinions. The Court can and should leave the work of "impos[ing] detailed restrictions on electronic surveillance" to Congress, as it has done before. *Ri-*

---

[24] https://www.epic.org/privacy/justices/alito/princeton/.

ley, 134 S. Ct. at 2497. But the Court should first establish that the Fourth Amendment applies to cell phone location data. It is "emphatically the province and duty of the judicial department to say what the law is." *Marbury v. Madison*, 5 U.S. 137, 177 (1803).

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to reverse the decision of the U.S. Court of Appeals for the Sixth Circuit.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

August 14, 2017